产品简介

McAfee Deep Defender

通过超越操作系统的安全防护来揭露并消除隐蔽的威胁

要点

- 内核级行为监控可揭露并删除未知威胁（包括 Rootkit）以抵御零日恶意软件
- 与位于内存和操作系统之间的 Intel 组件完美集成，执行实时内存和 CPU 监控
- 通过 McAfee ePO 软件进行管理，实现高效部署、集中式策略管理、增强的威胁监控以及统一报告
- 删除基于操作系统的传统防护手段无法检测到的低级威胁，降低重新映像和补救成本，增强整体安全性
- 隐匿恶意软件不断升级：McAfeeLabs™ 每个季度识别近 110000 种新型独特 Rootkit

“关于 Stuxnet 和 Zeus 等隐秘的恶意软件，要了解的最重要的一点在于这种恶意软件能真正控制其接管的计算机。通过在用户、内核和固件级别运行的 Rootkit，恶意软件能够进行自我隐藏、复制，并保护自身不受覆盖，导致病毒防护及其他防御手段失去效用。”

—David Marcus（McAfee Labs 和 Thom Sawicki (Intel)，隐匿犯罪软件领域的新现实，http://www.mcafee.com/cn/resources/white-papers / wp-reality-of-stealth-crimeware.pdf

隐匿恶意软件已成为网络犯罪分子的首选工具，越来越多的新型未知恶意软件采用 Rootkit 等伪装技术。犯罪分子依靠此类低级代码来逃避基于操作系统（OS）的防护。McAfee Deep Defender 利用 McAfee DeepSAFE 技术所支持的新一代硬件辅助安全防护，帮助您奋力还击。这种实时内核操作行为监控功能可揭露并删除高级隐蔽攻击。McAfee Deep Defender 与 McAfee ePolicy Orchestrator（McAfee ePO）软件和 McAfee Global Threat Intelligence（McAfee GTI）完美集成，轻松地将系统安全防护扩展到操作系统（OS）之外，以抵御隐蔽的零日威胁。

企业终端极易遭受隐匿恶意软件的攻击，因为它们能够绕过病毒防御以及基于操作系统的其他防御手段。犯罪分子设计这种低级恶意软件，企图利用操作系统的这一固有的安全弱点，隐藏自身形迹，致使系统在启动时觉察不到任何异常。

这种隐形恶意软件会肆意传播感染、停用对策以及窃取网络凭据或机密信息。恢复受害终端需要进行完全重新映像，每个事件都会占用 IT 人员和最终用户数小时时间，导致他们无法正常工作。

超越操作系统的防护

迈克菲与 Intel 共同研发了基于硬件的防护产品来抵御这些攻击，这种保护措施运行于 CPU 和操作系统之间，可保护位于物理内存中的各种组件。McAfee Deep Defender 能够在驱动程序及其他软件运行时进行可靠的监控，以便检测操作系统内部及其前后的威胁并予以清除。

实时内存和 CPU 监控

McAfee Deep Defender 利用 McAfee DeepSAFE® 技术（在 VMX 根模式下执行的内存软件层）提供实时内核内存和 CPU 事件保护，最大限度地降低对性能的影响。

这种低级监控功能可供 McAfee Deep Defender 识别隐匿恶意软件所采用的检测逃避技术，支持管理员实时监控内存进程，实施可配置的阻止或拒绝操作。如果 Rootkit 或隐匿恶意软件处于活动状态，McAfee DeepSAFE 将捕获尝试修改内核的活动。

真正的零日防护

McAfee Deep Defender 无需事先获悉 Rootkit 即可检测到它的存在。同时，McAfee Deep Defender 可识别 Rootkit 的恶意行为，从而提供真正的零日防护。

McAfee Deep Defender 能够在 Rootkit 试图隐藏恶意软件之前提供防护。其内核和内存防护包括：

- 阻止并记录对系统中断描述符表（IDT）和系统服务调度表（SSDT）执行的写入尝试
- 阻止对处理器系统转换表的更改
- 防止对直接内核对象操作（DKOM）列表和线程的修改
- 消除针对内核模式驱动程序的恶意附件
- 禁止嵌入式恶

系统要求和规格

- 支持 Intel Core i3、i5 和 i7 处理器
- 支持 Microsoft Windows 7（32 位和 64 位）
- 2 GB 内存(32 位)或 4GB 内存(64 位)
- 由 McAfee ePO 软件 4.5 或更高版本管理
- BIOS 支持的 Intel 虚拟化技术（VT，Virtualization Technology）
- 已完成国际化和本地化，可供全球部署

已针对与下列迈克菲产品的兼容性进行了测试：

- McAfee VirusScan Enterprise 8.7 或更高版本
- McAfee Application Control 5.x
- McAfee Endpoint Encryption for PC 5、5.2.6、5.2.9 和 6.1
- McAfee Host DLP 9.x
- McAfee Host Intrusion Prevention 8.x
- McAfee Network Access Control 3.2

- 阻止对驱动程序的导入地址表（IAT）挂接进行恶意修改
- 防止对内核导出地址表（EAT）进行恶意修改
- 阻止设备驱动程序执行恶意 I/O 调用
- 检测对驱动程序的调度例程进行的恶意更改

利用 McAfee GTI 检测并删除已知和未知威胁

McAfee Deep Defender 将报告、阻止、隔离和删除内核中的已知和未知恶意软件。现有的 McAfee VirusScan Enterprise 恶意软件防护技术利用 McAfee Deep Defender 的查找功能全面清理受影响的用户模式组件。

对于疑似或未知的恶意软件，McAfee Deep Defender 会将代码的指纹发送到 McAfee GTI 网络进行报告并确认其特征。一经确认，该恶意软件的指纹便会加入 McAfee GTI 数据库，以便将即时保护范围扩展到启用了 McAfee GTI 的其他终端，包括您站点中的其他终端。

通过 McAfee ePO 进行集中管理

McAfee Deep Defender 无需增加管理费用即可增强现有防护。现在，运行迈克菲终端软件的 PC 和笔记本电脑，可以在企业范围内所有使用现有 McAfee ePO 代理和管理基础设施的支持的系统上部署 McAfee Deep Defender。

熟悉的 McAfee ePO 控制台简化了 McAfee Deep Defender 实时内存操作策略的制定过程。安装 McAfee Deep Defender 后，您的 McAfee ePO 显示板和报告将对隐藏的威胁进行监控。

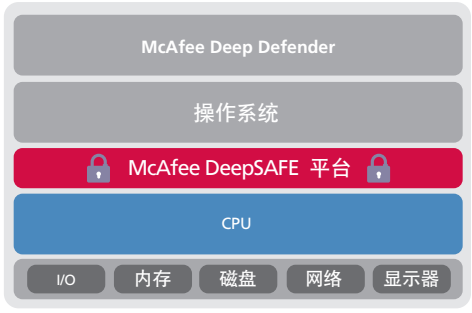

图 1. McAfee Deep Defender 利用 McAfee DeepSAFE 技术（位于 CPU 和操作系统之间）占据威胁监控的有利地位。

立即开始查找隐匿恶意软件

仅在操作系统内部运行的防御技术无法检测或揭露当今狡猾的网络犯罪分子采用的高级逃避技术。McAfee Deep Defender 采用关键增量防护技术来抵御这些威胁，弥补了传统终端安全防护的不足。

使用方便，因为 McAfee Deep Defender 充分利用了便捷的集中式 McAfee ePO 管理环境，加强了 McAfee VirusScan 防恶意软件引擎和 McAfeeGTI 网络提供的防护力度。

更多信息，请访问 www.mcafee.com/cn/deepdefender。

35301ds_deep-defender_1011_fnl_ETMG

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

迈克菲（北京）安全软件有限公司

北京市朝阳区建国路91号金地中心A座37楼	邮编：100022	电话：(8610) 85722000	传真：(8610) 86752299
上海市卢湾区湖滨路222号企业天地1号楼1101室	邮编：200021	电话：(8621)23080699	传真：(8621) 63406606
广州市天河区体育东路118号财富广场西塔15楼106室	邮编：510620	电话：(8620)38860668	传真：(8620) 38860638